Alaska Alternate Assessment

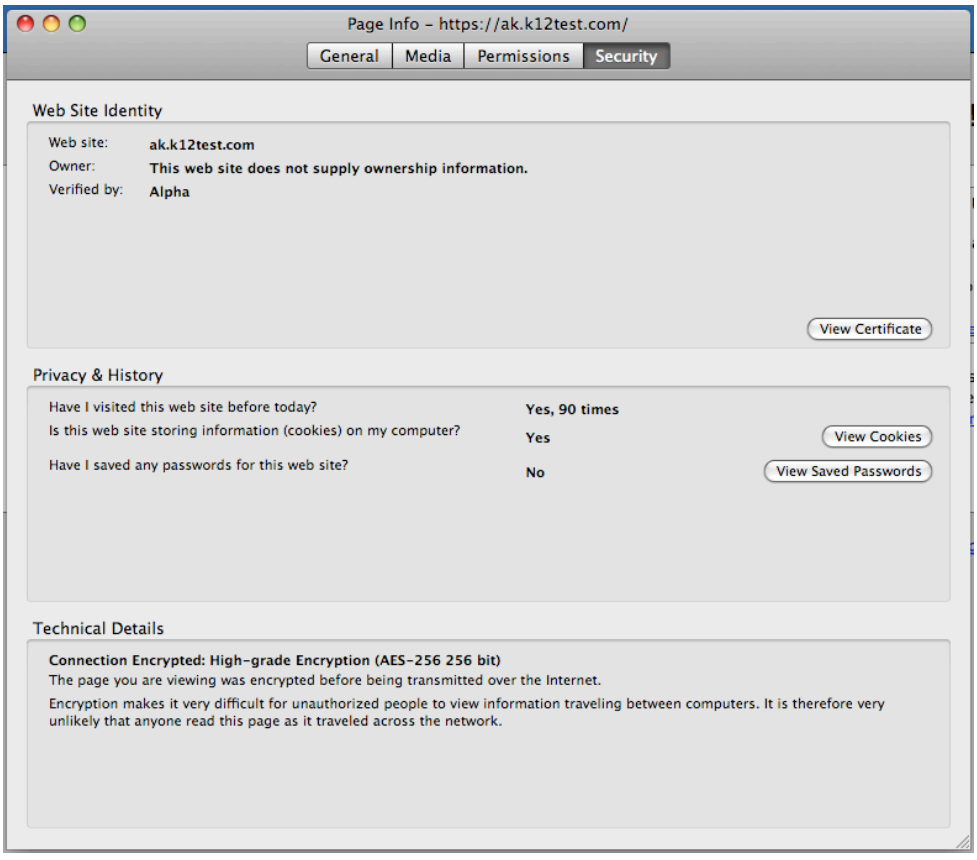
Website Security Assurances

June 2013

ISSUE 1: Secure access to http://ak.k12test.com

The AK website makes use of the cryptographic protocols Transport Layer Security (TSL) and Secure Socket Layer (SSL) to provide security from each end user's computer and the website's server. In order for this to work, a public key certificate has to be installed on the web server and signed by a trusted Certificate Authority (such as VeriSign or Alpha). Web browsers connect to the website over HTTPS using port 443, and after a series of handshakes using public and private keys, a secure connection is established. Basically any information sent from the website to a user's computer, and vice versa, is encrypted before being sent. This ensures protection from eavesdroppers and man-in-the-middle type attacks. The Site was made secure in August 2010.

ISSUE 2: Security of the website, the hosting servers, and transfer of secure data
To secure the AK website, a wildcard SSL certificate was purchased (for several hundred dollars) and installed on the web server. This uses Advanced Encryption Standard (AES) 256-bit high-grade encryption - the same level of encryption used by banks. Included in this report are several attachments which verify and document the security of the website. See below.



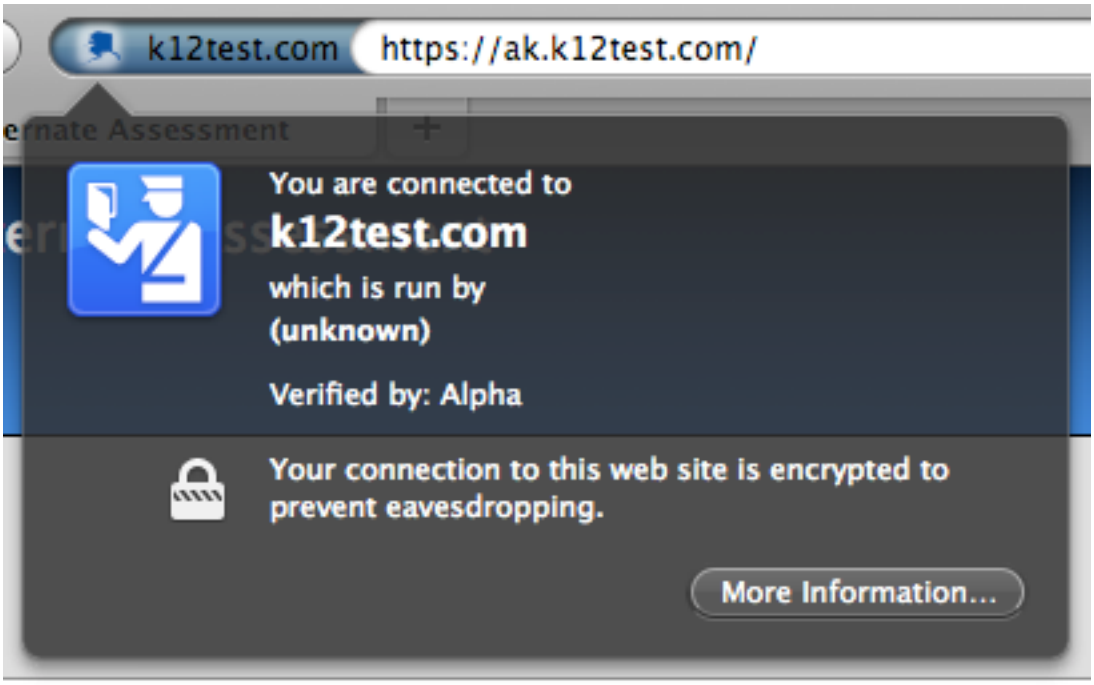
ISSUE 3: Security of the secure transfer site (filetrans.easycbm.com)

The Secure File Transfer Protocol (SFTP) server used for AK files (the "Fetch Server") uses a similar technology to that of the website (SSL), though it encrypts connections over port 22 instead of 443. Web servers can be configured to simultaneously listen for requests over the http:// protocol on port 80 as well as the https:// protocol on port 443, for increased compatibility with browsers, computers, and network settings. Based on previous feedback, the AK website was recently configured in this fashion to ensure successful mentor trainings, such as the one that took place last week, so that computer settings and network filters/configurations would not hamper the trainings. As these trainings have concluded, the web server has been configured to force all web traffic requests to come over HTTPS.

FTP servers such as our "Fetch Server" don't use http or https, but rather ftp and sftp instead. These are similar concepts, but different protocols and port numbers. Looking at Aran's copy/paste, it appears that she's using the File Zilla client, and the "Response: fzSftp" bit is showing that file zilla is using the Sftp protocol to connect. You can also see that 'open "akdoe@filetrans.easycbm.com" 22' is using port 22 (the standard port for SFTP), rather than port 21 (the port for plain FTP).

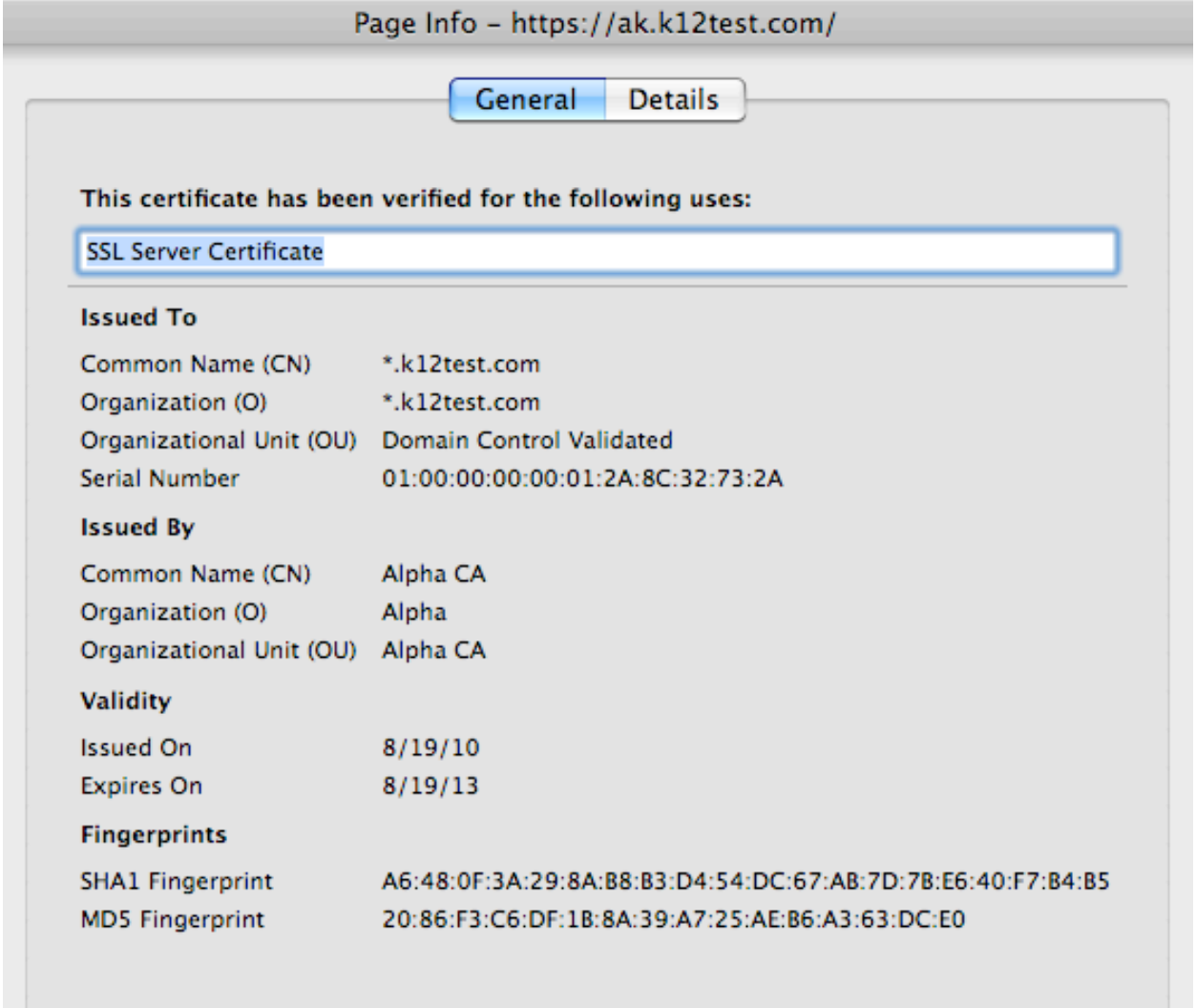
The hardware powering the AK website and SFTP wholly owned by Dillard Research Associates and collocated at a secure facility to allow user access. The colocation facility is certified reliable and secure, having received Statement on Auditing Standards No. 70 (SAS 70) Type II Certification and the SSAE16 attestation standard. This includes a full assessment of: Oversight by Executive Management, Operations and Customer Service, Development and Information Technology Organization, Human Resources Policies and Procedures, and Risk Assessment Monitoring. Such a review is important for service organizations, such as DRA, that provide services that are critical to its customers' operations - the SAS 70 Type II Certification provides third-party verification that, in turn, the organization's customers can supply for audits of their own operations (the audit meets Sarbanes-Oxley requirements). The server itself uses redundant drives in a RAID configuration, takes nightly backups of the database, and we keep offsite backups as well.

Firefox Reporting the encrypted connection:



Certificate Verification and Technical Details:

SSL Server Certificate with SHA1 and MD5 fingerprints:



Apache Directives enabling SSL on the server:

```
# Enable SSL
SSLEngine on
SSLCertificateKeyFile /etc/apache2/ssl/_.k12test.com.key
SSLCertificateFile /etc/apache2/ssl/_.k12test.com.crt
SSLCertificateChainFile /etc/apache2/ssl/AlphaSSLroot.crt
```